

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-278750

(43)Date of publication of application : 22.10.1996

(51)Int.Cl. G09C 1/00
G09C 1/00

(21)Application number : 08-048725 (71)Applicant : INTERNATL BUSINESS MACH
CORP <IBM>

(22)Date of filing : 06.03.1996 (72)Inventor : EASTER RANDALL J
MERZ WILLIAM A

(30)Priority

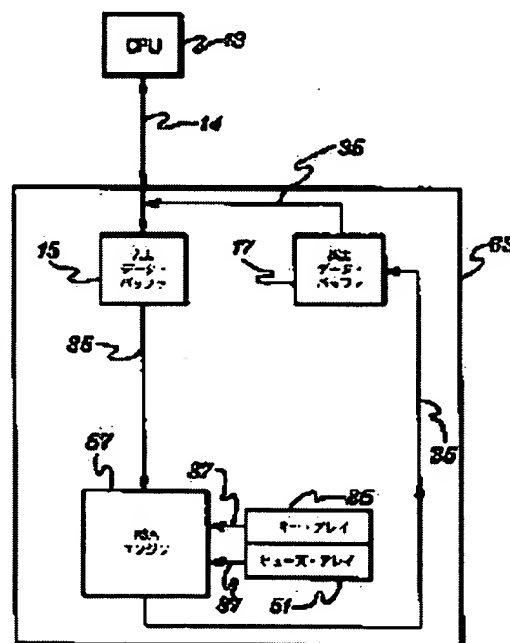
Priority number : 95 414852 Priority date : 31.03.1995 Priority country : US

(54) APPARATUS AND METHOD FOR ENCODING DATA USING PUBLIC KEY ENCODING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an apparatus and a method to encode data using a public key encoding method.

SOLUTION: An IC(integrated circuit) chip 63 having both of a public key encoding engine 57 and a fuse array 51 is prepared. The fuse array 51 is physically connected with the public key encoding engine 57 and encoded by a private key used by the encoding engine 57. Before the IC chip 63 is capsulated, the fuse array 51 is encoded by a laser abrasion process. After the IC chip is capsulated, the private key is permanently sealed in the IC chip 63 and kept secretly. Public key hash values and serial numbers may be encoded in the fuse array 51.



LEGAL STATUS

[Date of request for examination] 23.07.1998

[Date of sending the examiner's decision of rejection] 02.12.2002

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平8-278750

(43)公開日 平成8年(1996)10月22日

(51)Int.Cl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
G 0 9 C 1/00	6 3 0	7259-5 J	G 0 9 C 1/00	6 3 0 A
	6 6 0	7259-5 J		6 6 0 A

審査請求 未請求 請求項の数17 O L (全 10 頁)

(21)出願番号 特願平8-48725

(22)出願日 平成8年(1996)3月6日

(31)優先権主張番号 4 1 4 8 5 2

(32)優先日 1995年3月31日

(33)優先権主張国 米国 (U S)

(71)出願人 390009531

インターナショナル・ビジネス・マシーンズ・コーポレーション

INTERNATIONAL BUSINESS MACHINES CORPORATION

アメリカ合衆国10504、ニューヨーク州アーモンク (番地なし)

(72)発明者 ランダル・ジャイ・イースター

アメリカ合衆国12570、ニューヨーク州ボークアグ、ドッジ・ストリート 8

(74)代理人 弁理士 合田 潔 (外2名)

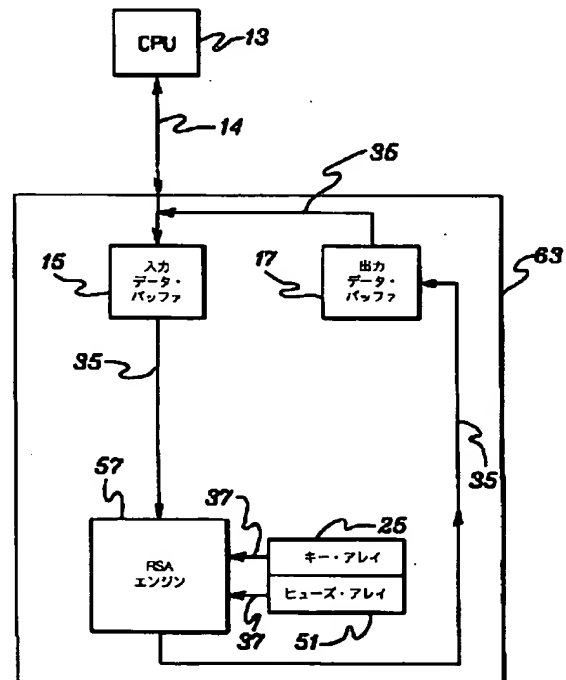
最終頁に続く

(54)【発明の名称】 公開キー暗号法を用いたデータ暗号化の装置及び方法

(57)【要約】

【課題】 公開キー暗号法を用いてデータを暗号化する装置及び方法を提供する。

【解決手段】 公開キー暗号エンジンとヒューズ・アレイの両方を持つI C (集積回路) チップが準備される。ヒューズ・アレイは公開キー暗号エンジンに物理的に接続され、暗号エンジンによって用いられる私用キーでエンコードされる。I C チップのカプセル化の前に、ヒューズ・アレイはレーザ・アブレーション・プロセスによりエンコードされる。カプセル化の後、私用キーがI C チップ内に永久的に封止され守秘される。ヒューズ・アレイには公開キー・ハッシュ値とシリアル番号をエンコードしてもよい。



1

【 特許請求の範囲】

【 請求項1 】 暗号装置に用いるI Cチップであって、私用キーを格納した不揮発性メモリと、前記不揮発性メモリに接続され、動作時に前記私用キーを使用する公開キー暗号エンジンと、を含む、I Cチップ。

【 請求項2 】 前記不揮発性メモリはヒューズ・アレイを含み、前記私用キーは前記I Cチップの生産時に前記ヒューズ・アレイにエンコードされる、請求項1記載の装置。

【 請求項3 】 前記不揮発性メモリに、公開キーを表す値がエンコードされた、請求項1記載の装置。

【 請求項4 】 前記値は公開キー・ハッシュ値を含む、請求項3記載の装置。

【 請求項5 】 前記不揮発性メモリに、前記私用キーに対応したシリアル番号がエンコードされた、請求項1記載の装置。

【 請求項6 】 前記I Cチップは、前記公開キー暗号エンジンに接続されて前記公開キーを格納するプログラマブル・メモリを含む、請求項1記載の装置。

【 請求項7 】 前記不揮発性メモリはヒューズ・アレイを含み、前記私用キーは前記I Cチップの生産時に前記ヒューズ・アレイにエンコードされ、前記ヒューズ・アレイに、前記公開キーの検査に用いられる前記公開キー・ハッシュ値がエンコードされた、請求項1記載の装置。

【 請求項8 】 暗号装置で私用キーを設定する方法であって、

a) 公開キー暗号エンジンと不揮発性メモリを持ち、前記公開キー暗号エンジンが前記不揮発性メモリに接続されたI Cチップを準備するステップと、

b) 私用キーを前記I Cチップの前記不揮発性メモリにエンコードするステップと、を含む、方法。

【 請求項9 】 前記不揮発性メモリはヒューズ・アレイを含み、前記エンコード・ステップb) は前記私用キーを前記ヒューズ・アレイにエンコードするステップを含む、請求項8記載の方法。

【 請求項10 】 前記エンコード・ステップb) はレーザ・アブレーションによって行なわれる、請求項9記載の方法。

【 請求項11 】 前記エンコード・ステップb) は、公開キーを表す値を前記不揮発性メモリにエンコードするステップを含む、請求項8記載の方法。

【 請求項12 】 前記公開キーを表す前記値は、前記エンコード・ステップb) が公開キー・ハッシュ値を前記不揮発性メモリにエンコードするステップを含むように、前記公開キー・ハッシュ値を含む、請求項11記載の方法。

【 請求項13 】 前記公開キー・ハッシュ値は前記公開キーの検査に用いられる、請求項12記載の方法。

2

【 請求項14 】 前記エンコード・ステップb) は、シリアル番号を前記不揮発性メモリにエンコードするステップを含む、請求項8記載の方法。

【 請求項15 】 前記準備ステップa) は前記I Cチップをカプセル化されていない状態で準備するステップを含み、前記方法は更に、前記I Cチップを前記エンコード・ステップb) の後にカプセル化するステップを含む、請求項8記載の方法。

【 請求項16 】 提示された前記公開キーを、前記公開キー暗号エンジンを持つI Cチップにロードするオペレーションを改良する方法であって、

a) 前記公開キー暗号エンジンと前記不揮発性メモリを持ち、前記公開キー暗号エンジンは前記不揮発性メモリに接続され、前記不揮発性メモリには所定の公開キーを表す値が格納された、I Cチップを準備するステップと、

b) 前記提示された公開キーのロード・オペレーションが改良されるように、前記提示された公開キーを、前記所定の公開キーを表す前記値に照らして検査するステップと、を含む、方法。

【 請求項17 】 前記準備ステップa) は公開キー・ハッシュ値が格納された前記I Cチップを準備するステップを含み、前記検査ステップb) は前記提示された公開キーを前記公開キー・ハッシュ値に照らして検査するステップを含むように、前記所定公開キーを表す前記値は前記公開キー・ハッシュ値を含む、請求項16記載の方法。

【 発明の詳細な説明】

【 0001 】

【 発明の属する技術分野】 本発明は、一般的にはデータの暗号化に関し、特に公開キー暗号法(public key cryptography)を用いたデータ暗号化の装置及び方法に関する。

【 0002 】

【 従来の技術】 コンピュータが毎日の業務に深く関わるようになり、処理された情報の安全性を守ることがこれまで以上に重要になっている。このような機密の必要性は、企業、政府、及び個人等を含めて多くのタイプの情報に当てはまる。そのためそうした情報の暗号化は有用ではあるが、暗号化装置であっても完全に安全というわけではない。従って、暗号化装置の整合性、及び保全性を改良する手法が求められる。

【 0003 】 一般的なデータ暗号化法は、米国標準局によって採用されているDES (データ暗号化規格) である。DES は比較的安全で低コストなデータ暗号化処理を実現するが、DES ベースの機器の管理面には問題がある。具体的には、DES ベースの暗号化機器で暗号化キーを管理する手法に問題がある。

【 0004 】 DES の暗号化法は秘密マスタ・キーを基

10

20

30

40

50

3

にしている。このマスタ・キーが2 者によって用いられるとき、2 者は互いの情報を支障なく暗号化し解読できるが、新しいマスタ・キーを通信相手に配付することに関して問題が生じる。従来の配付法には、新しいマスタ・キーを委任を受けた相手に与えるものがある。相手は新しいマスタ・キーを各暗号化デバイスに手動入力する。しかし、いずれかの暗号化デバイスがリモートにあるか、多くの暗号化デバイスがある場合には、それぞれにマスタ・キーを手動入力するのはきわめて煩雑で時間がかかる。また、マスタ・キーを個人に公開することに伴うリスクもある。他のキー配付法として、安全ではない通信リンクを通してキーを暗号化デバイスに転送するものがあるが、安全ではないキー配付が許容できないことは明らかである。

【0005】前記に代わる暗号化法として公開キー暗号法がある。この手法によると、ユーザは、最初に共通の秘密マスタ・キーを交換せずに暗号化情報を交換できる。具体的には、各ユーザは、個別の公開キー("K_p") と個別の私用(individual private) キー("K_s") の両方を持つ。公開キーは、全てのユーザとそれぞれの公開キーの共通データベースから取得できる(データベースは通常は、"キー・マネージャ" と呼ばれる中央コンピュータ装置に維持される)。私用キーは、従来は、ユーザがローカル・システムに手動入力するか、或いは私用キーが格納されたリムーバブル・データ・カードを差し込むことで入力されていた。

【0006】送信側ユーザは公開キー暗号化装置の動作中、最初にメッセージが送られる受信側ユーザを選ぶ。送信側ユーザは次に受信側ユーザの公開キーをチェックするため、キー・マネージャにリモートでアクセスし、選択されたユーザの公開キーを使ってメッセージを暗号化し、そのメッセージを送る。受信側ユーザはそこで、自身の私用キーを使ってメッセージを解読する。公開キー暗号化法は、送信側ユーザが受信側ユーザの公開キーを使って対応する私用キーを解読できないように"片道"機能を使用する。公開キー装置は以前からあり周知の通りである。例えばRivestらによる"A Method for Obtaining Digital Signatures and Public Key Cryptography", Comm. ACM, Vol. 21, No. 2(February 1978) では、Rivest, Shamir, 及びAdelman("RSA") の公開キー暗号化装置について説明されている。

【0007】公開キー暗号化装置は通常、DES 装置よりも低速であり、多くのデータ処理装置で使用することができない。解決法としては、長期的なデータ処理に用いられる比較的古いDES 型の装置用にキーを配付するために、公開キー装置を短期的に使用することが提案されている(前記引用文献を参照)。しかし公開キー装置のキー管理面では依然として問題が残る。

【0008】

【発明が解決しようとする課題】具体的には、上述のよ

4

うに、私用キーは各ユーザのために安全に維持することが望ましいが、それではDES に関して述べた問題、すなわち私用キーの安全をどのように守るかという、前記のものと同じ安全上の問題が生じる。解決法としては、私用キーが格納されたROM(読出し専用メモリ) を持つプラグイン・カードが提案されているが、これはデコードされたり、紛失したり、或いは盗まれたりする可能性がある。また安全ではない私用キーの転送も同じように許容できない。従って、私用キーを設定するより安全な手法が求められる。

【0009】

【課題を解決するための手段】本発明は前記の問題を解決するためのものである。

【0010】本発明は、第一の側面として、暗号化装置に用いるIC(集積回路) チップを含む。ICチップは、私用キーを格納した不揮発性メモリを含む。またICチップには、不揮発性メモリに接続された公開キー暗号化エンジンが含まれる。特に公開キー暗号化エンジンは動作時に公開キーを使用する。

【0011】改良点として、不揮発性メモリはヒューズ・アレイを含む。具体的には、私用キーはICチップの生産時にヒューズ・アレイにエンコードできる。ヒューズ・アレイもまた、例えば公開キー・ハッシュ値とシリアル番号でエンコードできる。

【0012】本発明は、他の側面として、暗号化装置で私用キーを設定する方法を含む。この方法は、ICチップに、上述の公開キー暗号化エンジンと不揮発性メモリを付加するステップを含む。また私用キーはICチップの不揮発性メモリにエンコードされる。不揮発性メモリがヒューズ・アレイを含む場合には、エンコードはレーザ・アブレーションにより行える。他の方法及び装置もここに開示している。

【0013】まとめると、本発明の手法は、多くの特徴及び利点により公開キー暗号化装置を改良するものである。出荷前、カプセル化の前に、私用キーをICチップに、不揮発性としてエンコードすることで、私用キーの機密性が保証される。具体的には、私用キーを見つけようとする試みはどのようなものであれICチップを破壊する結果になる。また私用キーに不揮発性メモリを使用することにより、外部の手段でICチップに値をロードすることに伴う安全上の問題がなくなる。従って、例えば、DES 等の他の暗号化装置用のキーを安全に転送しロードする等、多くの用途を持つ、シングルICチップを用いた安全性の高い公開キー暗号化装置が得られる。

【0014】

【発明の実施の形態】本発明の手法は、高安全度、高性能の公開キー暗号装置の作成及び動作を改良するものである。具体的には、この暗号装置は、出荷前にエンコードされた私用キーを格納した不揮発性メモリと共に、シングルICチップに格納される。従って一度、出荷前に

10

20

30

40

50

5

エンコードされカプセル化されると、I Cチップを破壊することなく私用キーを発見する方法はない。従って、このシングルI Cチップ暗号装置(シングル・チップ装置) は、米商務省がF I P S P U B 1 4 0 - 1として1 9 9 4年1月11日に発表した"SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES(暗号モジュールの安全要件)"規格に準拠した最上位の安全認定レベルを達成している。

【0015】シングル・チップ装置の不揮発性キー記憶領域は他の面でも役立つことに注意されたい。例えば、(出荷前にプログラミングされた私用キーに対応する) 公開キーに対応した値を、私用キーに加えて出荷前に不揮発性メモリにエンコードすることができる。また、シングル・チップ装置のプログラマブル記憶領域は、公開キーを格納するよう指定できる。シングル・チップ装置の動作を初期化する際、ロードされている公開キーを、公開キーに対応した出荷前のエンコードされた値に照らして調べることで、正しい公開キーが用いられているか確認することができる。

【0016】本発明の手法は、これまでの暗号装置と一緒に用いることができる。例えば、従来の暗号化エンジン(DES暗号化エンジン等) のキーの安全な転送及びロードを改良する公開キー暗号装置を提供するために用いることができる。

【0017】一般的な背景情報として、従来のキーを手動ロードするDES暗号化装置を図1に示している。I C R F T C M(Integrated Cryptographic Resource Facility Thermal Conduction Module、統合暗号リソース機構伝熱モジュール) 11がCPU(中央処理装置) 13とKSU(キー記憶ユニット) 29に接続される。CPU13は、例えば、バス14を通したI C R F T C M11の接続については周知のIBM ES/9000アーキテクチャ処理装置等である。またKSU29についても周知の通りであり、安全ケーブル27を通してI C R F T C M11に接続される。これらのエンティティは、改竄を検出し応答を返す、物理的に安全なハードウェアによって保護される。

【0018】KSU29はマスタ・キーを記憶するメモリを提供する。具体的には、KSUがマスタ・キーの部分を受け入れられる状態のモードにすることによってマスタ・キーが入力される。ユーザはそこで、物理キー(brass key) 31を差し込むと共に、16進キー・パッド33を使ってマスタ・キーの部分を手動入力する。

【0019】I C R F T C M11は、DESベースの暗号化エンジンに必要な機能要素を共に実現する複数のI Cチップを含む。具体的には、入力バッファ15と出力バッファ17が、内部バス35とCPUバス・ライン14を通してCPU13へのデータの入力/出力を調整する。暗号エンジンすなわちDESエンジン21は、バス35のデータ・バス内に置かれ、データの暗号のエン

6

コード及びデコードが改良される。最後に、キー管理は、KSUインタフェース23、DESマスタ・キーを記憶するための揮発性キー・アレイ25、及びキー転送バス37の組み合わせによって実現される。

【0020】この装置の手動キー入力機能にはいくつかの欠点がある。特にKSU29への物理的なアクセスは難しい。具体的には、コンピュータ装置はしばしばモートにあり、物理的なアクセスが容易ではない。また、複数の装置があると、キー管理に必要な人的資源が増える。更に、DESマスタ・キーの部分個人に公開する必要があるため、装置全体の安全性が低下する。従って、より安全で管理しやすいキー配付装置が求められる。

【0021】前記の問題の解決法としては、公開キー暗号装置を使用してDES装置のキー配付を改良する方法がある。この点については、本発明の実施例として、シングルI Cチップ公開キー暗号装置63を実現することができる(図2)。図2では同じ参照符号を用いて図1からの同様な機能要素を示している。

【0022】シングルI Cチップ装置63は、内部バス35とI/Oバス14を通してCPU13でI/Oを制御する入力バッファ15と出力バッファ17を含む。公開キー暗号エンジンとしてRSAエンジン57がある。これらの要素は全てバス35によって相互接続される。また、キー転送バス37を通してRSAエンジン57に接続されたヒューズ・アレイ51とキー・アレイ25の組み合わせによりキー記憶域が得られる。

【0023】キー・アレイ25とヒューズ・アレイ51の組み合わせによってRSAエンジン57のキー記憶機構が得られる。公開キー暗号エンジン(RSAエンジン57等) は私用キー及び公開キーを使用する必要がある。私用キーは、本発明に従って、ヒューズ・アレイ51を含む不揮発性メモリ内に格納され、公開キーは、キー・アレイ25を含む揮発性メモリ(RAM等) にロード可能である。

【0024】更に説明を加えると、公開キー装置用の私用キーの安全な記憶域を確保することは、これまで長い間難しいタスクであった。様々な手法が試されているが、きわめて高い安全性を達成したものはない。例えばMunckらによる1988年2月2日付米国特許番号第4723284号、"AUTHENTICATION SYSTEM"では、私用キーはリムーバブルROMカードに格納される。これには盗難、紛失、或いはデコードの恐れがある。ある装置の私用キーは、本発明の手法によれば、出荷前、カプセル化の前に、シングルI Cチップ63のヒューズ・アレイ51にエンコードされる。従って、I Cチップがカプセル化された後は、I Cチップ自体を破壊しない限り私用キーの検出は不可能である。

【0025】このようなI Cチップを生産するために必要な個々の処理ステップは当業者には明らかであろう。

10

20

30

40

50

公開キー及び私用キーの揮発性記憶域を持つシングル・チップRSA装置は一般に数多く出回っている。例えばデンマークのJydks TelefonのRSAチップがある。この広告用パンフレットには"全く新しい世界記録に対する権利が手に入る"とある。ただしこのようなチップには、動作時に外部のソースから私用キーをロードしなければならないという前記の安全上の問題がある。ヒューズ・アレイ51は、本発明の手法に従って、従来の揮発性キー記憶手段の代わりに生産時にICチップに組み込まれる。

【0026】ヒューズ・アレイは、当業者には明らかなように、CMOS（相補型金属酸化膜半導体）プロセス等のICチップ生産プロセスのパーツとして周知の通りである（例えばMassachusetts Institute of Technology Lincoln LaboratoryのJ. I. Raffelによる"Restructurable VLSI Using Laser Cutting and Linking", SPIE/LA 1983を参照）。ヒューズ・アレイ51は、本発明の原理に従って、例えば私用キー、シリアル番号、及び対応する公開キー・ハッシュ値を格納するのに用いられる。

【0027】ICチップ63をエンコードするプロセスを図3のフローチャートにまとめている。ICチップ63にRSAエンジン57とヒューズ・アレイ51が付加される（ステップ71）。このICチップは自製でき、あるいは外部から供給を受けてもよい。次に、ICチップ用に私用キーと公開キーのペアが指定される。本発明に従って、ヒューズ・アレイが私用キーでエンコードされる（ステップ73）。更にヒューズ・アレイは、対応する公開キー・ハッシュ値（ステップ75）及びシリアル番号（ステップ76）でエンコードされる。エンコードのステップは以下に詳しく説明する。

【0028】更に具体的には、公開キーにハッシュ関数が適用されて、対応する公開キー・ハッシュ値が決定される。ハッシュ関数の1例としてMDC4（変更検出コード4）関数がある。Rivestによる"The MD4 Message-Digest Algorithm", Network Working Group RFC 1320 of the MIT Laboratory for Computer Science and RSADa Data Security, April 1992にMDC4関数を実行する方法が記載されている。従って、MDC4関数は公開キーに適用され、ヒューズ・アレイにエンコードされる対応するハッシュ値が決定される。他のクラスの関数もハッシュ関数に代えられることに注意されたい。基本的には、入力として公開キーを受け入れ、それを表す値を出力とする関数であれば使用できる。ハッシュ関数はこのような関数の1例にすぎない。

【0029】更に、公開キーと私用キーのペアに対応したシリアル番号がヒューズ・アレイ51にエンコードされる。シリアル番号は、キー・マネージャで例えば対応する公開キーを調べるために用いられる公開値である。例えば、ある装置の公開キーは、装置にそのシリアル番

号を照会し、対応する公開キーを取得するためにシリアル番号をキー・マネージャに示すことによって取得できる。

【0030】ヒューズ・アレイをエンコードするプロセスは当業者には明らかであろう。1例を挙げると、レーザ・アブレーション・プロセスにより、ヒューズ・アレイの指定された可融リンクを選択的に遮断することができる（先に引用したRaffelの文献を参照）。例えば、遮断されたリンクは2進0を表わし、遮断されていないリンクは2進1を表すことができる。従って公開キー・ハッシュ値、私用キー、及びシリアル番号はそのようにエンコードできる。

【0031】エンコードの後、ICチップ63はカプセル化され、回路に組み込める状態になる。この段階で、私用キーの値が完全に守秘されるように、私用キーの記録は全て破棄できる。実際、カプセル化されたICチップを取り外してヒューズ・アレイの設定を見つけようとしても、大抵はICチップを破壊する結果になる。そのため、このICチップは、ここに述べているFIPS140-1規格に従った安全性ランキングの最上位のレベルを取得している。

【0032】先に述べた通り、公開キー・ハッシュ値は、キー・アレイにロードする公開キーの検査が改良されるように、ヒューズ・アレイにエンコードされる。更に説明を加えると、ICチップ63の動作の初期化時に、公開キーをキー・アレイ25（図2）にロードするのが望ましいが、その前に公開キーが正しいか検査することもまた望ましい。例えば、提示された公開キーのハッシュ値を計算し、それを出荷前にエンコードされた所定の公開キー・ハッシュ値と比較することで、提示された公開キーの検査が改良される。

【0033】以下、公開キー検査プロセスを図4のフローチャートに関してまとめる。最初、提示された公開キーが取得され、シングルICチップ63のキー記憶アレイ25にロードされる（図2）。このキーは、例えばキー・マネージャから検索できる。提示された公開キーは次にICチップ63に転送され、そこでそのハッシュ値が計算される（ステップ77）。ICチップ上のMDC4アルゴリズム等のハッシング・アルゴリズムのハードウェアが計算に用いられる。例えばMDC4アルゴリズムをハードウェアで実現することは、RivestのMDC4アルゴリズム、或いは以下の回路例（図6）を見れば当業者には明らかであろう。提示された公開キーについて確認されたハッシュ値は次に、ヒューズ・アレイに格納されたハッシュ値と比較される（ステップ79）。結果が良ければ、確認された提示公開キーがキー・アレイ25にロードされる（ステップ81）。結果が否定的であれば、オペレーションはリトライされるか中止され（ステップ83）、対応するシステム・レベルが指示される。

10

20

30

40

50

【0034】MDC4 関数のハードウェアを図6に示す。具体的にはマルチステージ装置の1つのステージが示してある。全体で、64ビットのデータ・ブロック n 個($n \geq 1$)について単一MDCが複数のステージによって計算される。このステージは64ビットのデータ・ブロック X_i を受け入れる($1 \leq i \leq n$)。入力としてはまた、前のステージの出力に対応した $CV1(i)$ 及び $CV2(i)$ 、すなわちそれぞれ $OUT1(i-1)$ 、 $OUT2(i-1)$ が受け入れられる。図のMDC4装置はまた、そのセクション間の中間値を $KK1(i)$ 、 $KK2(i)$ として出力する。特にセクション100Aは $KK1(i)$ を出力し、 $KK1(i)$ はセクション100Cの入力になる。セクション100Bは $KK2(i)$ を出力し、 $KK2(i)$ はセクション100Dの入力になる。

【0035】MDC4ハードウェア装置のセクション100Aについて以下に詳しく説明する。他のセクションは機能的には同様であり、対応する参照符号で示している。セクション100Aで、入力 $CV(i)$ と'A'はOR要素101Aで論理和がとられる。'A'の値は例えばMDC4関数で16進4000000000000000である。OR要素101Aの出力はAND要素103Aに入力され、'B'との論理積がとられる。'B'の値は、例えばMDC4関数で16進DFFFFFFFである。AND要素103Aの出力はE要素105A(加算器)に入力され、 X_i の値に加算される。E要素105Aの出力はXOR要素107Aに入力され、 X_i の値との排他的論理和がとられる。XOR要素107Aからの結果はレジスタ109Aに送られる。レジスタ109Aは左半分111A(ビット0乃至31)と右半分113A(ビット32乃至63)を含む。レジスタ109Aは、以下に述べるようにセクション100Bからのレジスタ109Bの値と組み合わせられる。

【0036】セクション100Bはセクション100Aと同様の構造を持つ。1つの違いとして、セクション100Aの $CV1(i)$ の代わりに入力として $CV2(i)$ が用いられる。また値'A'と'B'がそれぞれ値'C'と'D'に置き換えられる点も異なる。具体的には、例えば'C'はMDC4関数について16進2000000000000000からなり、'D'は16進BFFFFFFFである。これらの例外はあるが、OR要素101B、AND要素103B、E要素105B、XOR要素107B、及び左半分111Bと右半分113Bを持つレジスタ109Bは、セクション100Aのそれぞれの対応する要素と同様に機能する。

【0037】レジスタ109A及び109Bは、それらの値の組み合わせがレジスタ115A及びレジスタ115Bに格納されて、それぞれ $KK1(i)$ 、 $KK2(i)$ としてセクション100C、100Dに出力され

るようにクロス接続される。具体的には、レジスタ109Aの右半分113Aはレジスタ115Bの右半分119Bに接続され、レジスタ109Bの右半分113Bはレジスタ115Aの右半分119Aに接続される。レジスタ109Aの左半分111Aはレジスタ115Aの左半分117Aに接続され、レジスタ109Bの左半分111Bはレジスタ115Bの左半分117Bに接続される。つまり $KK1(i)$ 及び $KK2(i)$ の値はそれぞれレジスタ115A及び115Bに格納される。

【0038】MDC4装置の他の部分すなわちセクション100C及び100Dはそれぞれ上述のようにセクション100A、100Bと同様である。1つの違いとして入力に変更されている。具体的にはセクション100Cで、セクション100Aの $CV1(i)$ と X_i はそれぞれ $KK1(i)$ と $CV2(i)$ に置き換えられる。同様にセクション100Dで、セクション100Bの $CV2(i)$ と X_i はそれぞれ $KK2(i)$ と $CV1(i)$ に置き換えられる。また出力も異なっている。特にセクション100Cで出力は $OUT1(i)$ を含み、セクション100Dで出力は $OUT2(i)$ を含む。前記の違いを除けば、セクション100A、100Bの要素に関して、それぞれセクション100C、100Dの要素と比較して、同様な符号を付けた要素は同様な機能を持つ。

【0039】先に述べたMDC4装置の単一ステージは、当業者には明らかなように、処理に必要な全ステージを得るために反復可能である。従ってハードウェアベースのMDC4関数が実現される。ハッシュ値、または公開キーにもとづく同様の値を計算する他の関数も、シングルICチップのハードウェアに実現可能である。このような実現の詳細は当業者には明らかであろう。

【0040】本発明の手法の他の応用例として、本発明の公開キー暗号法を用いてDESマスタ・キーの配付を簡素化するDESベースの暗号化装置を作成できる(図5)。図5に示した装置は図1と似ているが、キーの手動ロードの全ての側面が公開キー暗号装置によって置き換えられている。またこの機能は全て、本発明に従ってシングルICチップ53に実現されている。

【0041】シングルICチップ53は、図1及び図2の装置と同様な多くの要素を含む。すなわち内部バス35とI/Oバス14を通してCPU13によりI/Oを制御する入力バッファ15及び出力バッファ17である。またDES暗号エンジン21がシングルICチップ53に実現されて暗号機能が得られる。更にRSAエンジン57が公開キー暗号エンジンとして付加される。各種暗号エンジンのキー記憶域は、ヒューズ・アレイ51とキー・アレイ25の組み合わせにより得られる。要素間のデータ・パスは内部バス35によって与えられ、キー転送はキー転送バス37で行なわれる。

【0042】DES暗号エンジン21のキーはキー・ア

レイ25に格納される。これは例えばRAMを含むプログラマブル記憶域である。動作時、キーはDESマスタ・キーとして用いられるよう、RSAエンジン57により公開キー暗号法を通して転送される。このような転送の手法としては先に引用したMunckらによるものがある。利点として、本発明の手法により、私用キーの安全性が確保され、従来のキーの手動ロード装置の欠点が克服される。

【0043】まとめると、本発明の手法は、多くの特徴と利点により公開キー暗号装置を改良するものである。出荷前、カプセル化の前に、私用キーをICチップに、永久的にエンコードすることで私用キーの機密性が保証される。この場合も、私用キーを見つけようとしてもICチップを破壊する結果になる。カプセル化されたヒューズ・アレイを使用することでこの面が強化される。また私用キー用に不揮発性オンチップ記憶域を用いることで、外部手段によりチップに私用キーの値をロードすることに伴う安全上の問題が解消される。従って、DES等、他の暗号装置用のキーの安全な転送とロードを含めて多くの用途のある、安全性の高いシングルICチップの公開キー暗号装置が得られる。

【0044】まとめとして、本発明の構成に関して以下の事項を開示する。

【0045】(1) 暗号装置に用いるICチップであって、私用キーを格納した不揮発性メモリと、前記不揮発性メモリに接続され、動作時に前記私用キーを使用する公開キー暗号エンジンと、を含む、ICチップ。

(2) 前記不揮発性メモリはヒューズ・アレイを含み、前記私用キーは前記ICチップの生産時に前記ヒューズ・アレイにエンコードされる、前記(1)記載の装置。

(3) 前記不揮発性メモリに、公開キーを表す値がエンコードされた、前記(1)記載の装置。

(4) 前記値は公開キー・ハッシュ値を含む、前記(3)記載の装置。

(5) 前記不揮発性メモリに、前記私用キーに対応したシリアル番号がエンコードされた、前記(1)記載の装置。

(6) 前記ICチップは、前記公開キー暗号エンジンに接続されて前記公開キーを格納するプログラマブル・メモリを含む、前記(1)記載の装置。

(7) 前記不揮発性メモリはヒューズ・アレイを含み、前記私用キーは前記ICチップの生産時に前記ヒューズ・アレイにエンコードされ、前記ヒューズ・アレイに、前記公開キーの検査に用いられる前記公開キー・ハッシュ値がエンコードされた、前記(1)記載の装置。

(8) 暗号装置で私用キーを設定する方法であって、
a) 公開キー暗号エンジンと不揮発性メモリを持ち、前記公開キー暗号エンジンが前記不揮発性メモリに接続されたICチップを準備するステップと、
b) 私用キーを前記ICチップの前記不揮発性メモリに

エンコードするステップと、を含む、方法。

(9) 前記不揮発性メモリはヒューズ・アレイを含み、前記エンコードのステップb)は前記私用キーを前記ヒューズ・アレイにエンコードするステップを含む、前記(8)記載の方法。

(10) 前記エンコードのステップb)はレーザ・アブレーションによって行なわれる、前記(9)記載の方法。

(11) 前記エンコードのステップb)は、公開キーを表す値を前記不揮発性メモリにエンコードするステップを含む、前記(8)記載の方法。

(12) 前記公開キーを表す前記値は、前記エンコードのステップb)が公開キー・ハッシュ値を前記不揮発性メモリにエンコードするステップを含むように、前記公開キー・ハッシュ値を含む、前記(11)記載の方法。

(13) 前記公開キー・ハッシュ値は前記公開キーの検査に用いられる、前記(12)記載の方法。

(14) 前記エンコードのステップb)は、シリアル番号を前記不揮発性メモリにエンコードするステップを含む、前記(8)記載の方法。

(15) 前記準備ステップa)は前記ICチップをカプセル化されていない状態で準備するステップを含み、前記方法は更に、前記ICチップを前記エンコード・ステップb)の後にカプセル化するステップを含む、前記(8)記載の方法。

(16) 提示された前記公開キーを、前記公開キー暗号エンジンを持つICチップにロードするオペレーションを改良する方法であって、

a) 前記公開キー暗号エンジンと前記不揮発性メモリを持ち、前記公開キー暗号エンジンは前記不揮発性メモリに接続され、前記不揮発性メモリには所定の公開キーを表す値が格納された、ICチップを準備するステップと、

b) 前記提示された公開キーのロード・オペレーションが改良されるように、前記提示された公開キーを、前記所定の公開キーを表す前記値に照らして検査するステップと、を含む、方法。

(17) 前記準備ステップa)は公開キー・ハッシュ値が格納された前記ICチップを準備するステップを含み、前記検査ステップb)は前記提示された公開キーを前記公開キー・ハッシュ値に照らして検査するステップを含むように、前記所定公開キーを表す前記値は前記公開キー・ハッシュ値を含む、前記(16)記載の方法。

【図面の簡単な説明】

【図1】キーを手動入力する従来の暗号化装置の図である。

【図2】本発明の実施例に従ったシングルIC(集積回路)チップの公開キー暗号化装置の図である。

【図3】本発明の実施例に従って、図2のシングルICチップ暗号化装置にキー情報をエンコードする方法のフ

13

ローチャートを示す図である。

【図4】本発明の実施例に従って、図2のシングルI Cチップ暗号化装置に公開キーをロードする方法のフローチャートを示す図である。

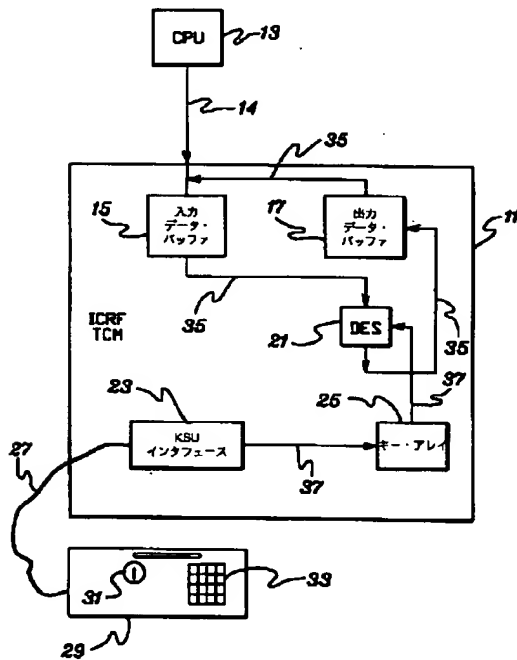
【図5】本発明の実施例に従って、DES暗号エンジンのマスタ・キーの転送を改良するために公開キー暗号法を用いる暗号装置の図である。

【図6】本発明の実施例に従ったMDC4(変更検出コード4)のハードウェア例を示す図である。

【符号の説明】

- 11 ICRF TCM
- 13 CPU
- 14 I/Oバス
- 15 入力バッファ
- 17 出力バッファ
- 21 DES暗号エンジン
- 23 KSUインタフェース
- 25 揮発性キー・アレイ

【図1】



14

27 安全ケーブル

29 KSU

31 物理キー

33 16進キー・パッド

35 内部バス

37 キー転送バス

51 ヒューズ・アレイ

53 シングルI Cチップ

57 RSAエンジン

10 63 シングルI Cチップ公開キー暗号装置

100A、100B、100C、100D セクション

101A、101B OR要素

103A、103B AND要素

105A、105B E要素

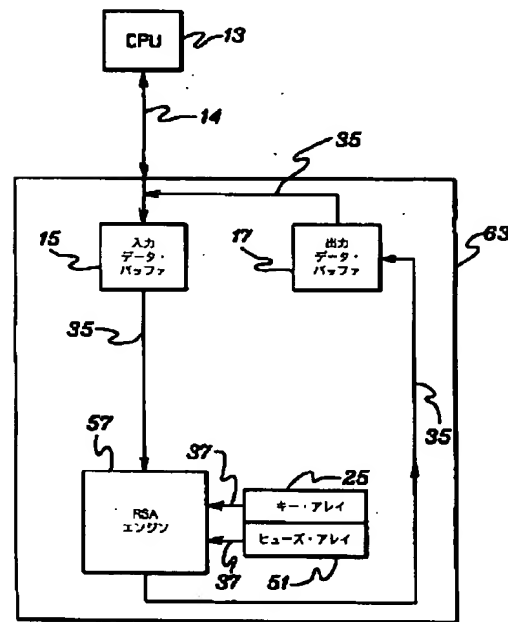
107A、107B XOR要素

109A、109B、115、115B レジスタ

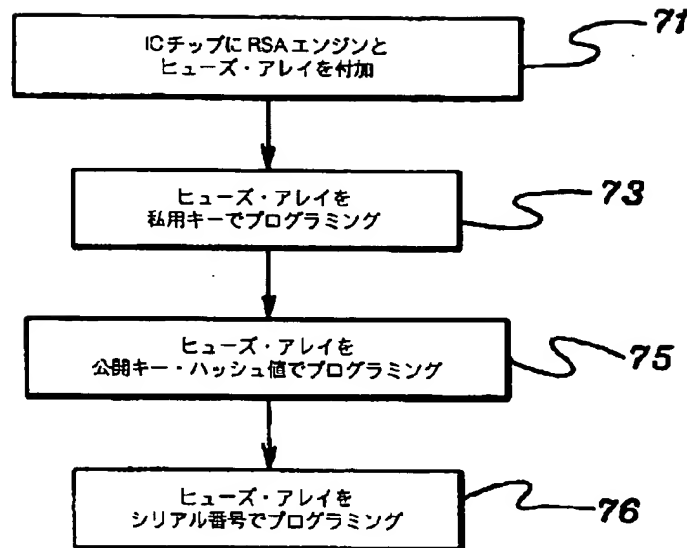
111A、111B 左半分

113A、113B 右半分

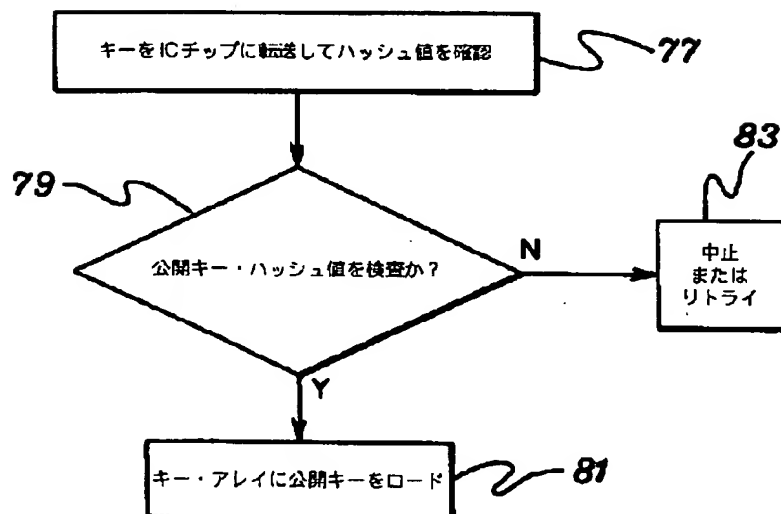
【図2】



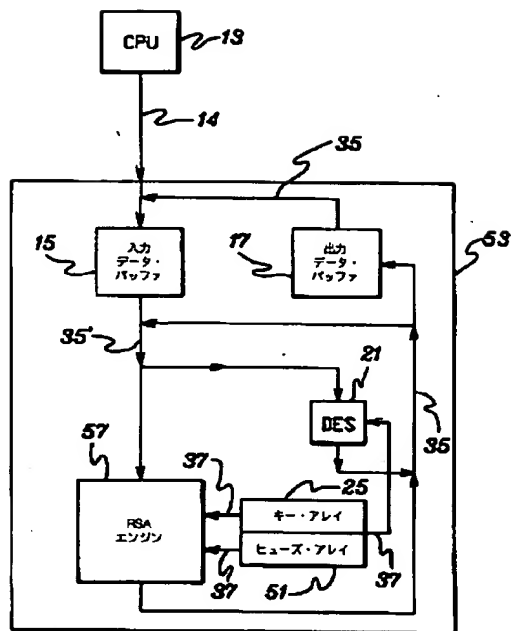
【 図3 】



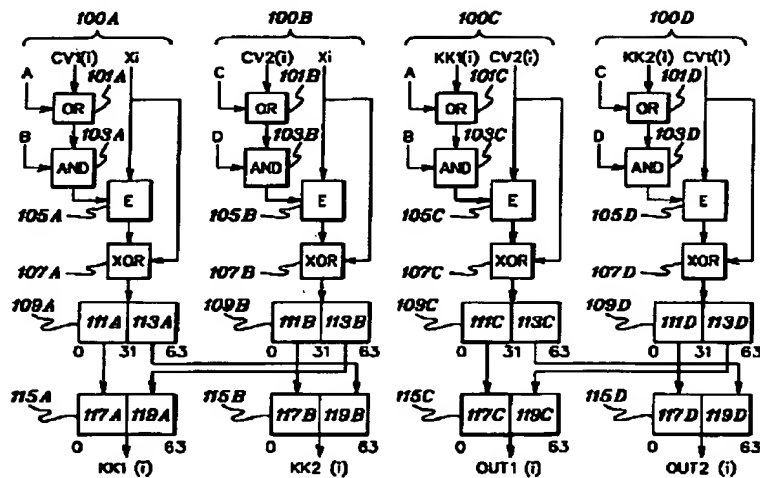
【 図4 】



【 図5 】



【 図6 】



フロント ページの続き

(72) 発明者 ウィリアム・オーガスト・メルツ
 アメリカ合衆国12590、ニューヨーク州ワ
 ッピングアーズ・フォールズ、マロニー・ド
 ライブ 28